National Cybersecurity Assessment and Technical Services

Updated: September 9, 2015

Homeland Security

NCATS Program Overview

- Offer Full-Scope Red Team/Penetration Testing Capabilities through two primary programs: **Risk and Vulnerability Assessment (RVA)** and **Cyber Hygiene**
- Focus is on proactive engagements with stakeholders to improve their cybersecurity posture, limit exposure, reduce rates of exploitation
- Offers a full suite of tailored threat, vulnerability and risk assessment services and penetration testing capabilities to stakeholders
- Acts as a trusted advisor and provides independent review and recommendations for cybersecurity improvement

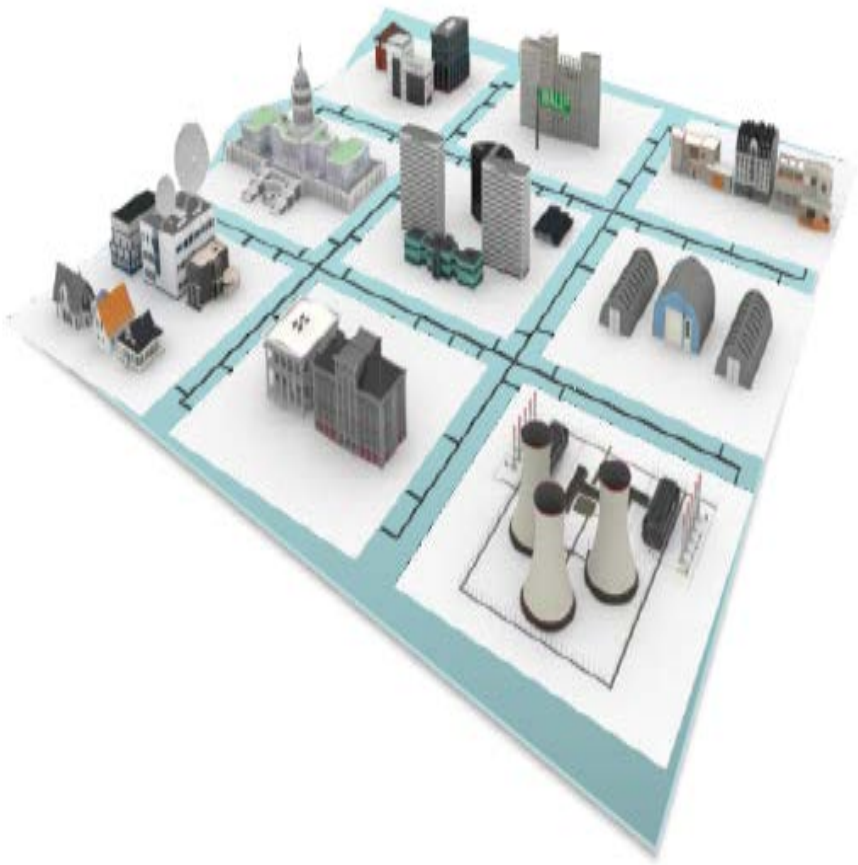
Objectives and Benefits

- Provide Enhanced Situational Awareness and Data Visibility to Leadership
  - Types of information:
    - Vulnerabilities
    - Mitigations
    - Operating Systems
    - Applications
  - Trending and Comparison Data
    - Federal, SLTT, PS

Stakeholder Groups

- Federal Civilian Executive Branch
- State, Local, Tribal, Territorial Government (SLTT)
- Private Sector (PS)
- Unclassified / Business Networks

- **Cyber Hygiene**
  - Mandatory for Federal
  - Optional for SLTT and PS
- **Risk and Vulnerability Assessments**
  - Optional for Federal, SLTT and PS



FY15 Current Stakeholders				
Service	**Fed**	**SLTT**	**PS**	**Total**
RVA	24	10	12	46
Cyber Hygiene	126*	35	22	183

* Includes House of Representatives

Services and Capabilities

Service	Description	Internal/ External to Customer Network	Program
Vulnerability Scanning	Conduct Vulnerability Assessments	Both	Cyber Hygiene RVA
Penetration Testing	Exploit weakness or test responses in systems, applications, network and security controls	Both	RVA
Social Engineering	Crafted e-mail at targeted audience to test Security Awareness / Used as an attack vector to internal network	External	RVA
Wireless Discovery & Identification	Identify wireless signals (to include identification of rogue wireless devices) and exploit access points	Internal	RVA
Web Application Scanning and Testing	Identify web application vulnerabilities	Both	Cyber Hygiene RVA
Database Scanning	Security Scan of database settings and controls	Internal	RVA
Operating System Scanning	Security Scan of Operating System to do Compliance Checks (ex. FDCC/USGCB)	Internal	RVA

RVA – Assessment Lifecycle

Pre ROE

- Stakeholder contacted
- Briefed on NCATS services
- Service is Requested
- Schedule Confirmed
- ROE Distributed/Stakeholder signs ROE

Pre Assessment

(Minimum) 2 weeks

- Pre-Assessment Package Distributed
- Receive Completed Pre-Assessment Package
- Conduct Pre-Assessment Teleconference
- Receive Pre-Assessment Artifacts (1 week)

Assessment

2 weeks

- Notification to NCCIC Floor for dissemination
- Off-Site Assessment Activities
- On-Site Assessment Activities

Reporting

3 weeks

- Draft Report Started/Completed
- Submit Draft Report to Stakeholder
- Receive Draft Report with Stakeholder Comments
- Q&A Process Started/Completed

Post Assessment

1 week

- Final Draft Completed
- Final Report Delivered to Customer
- Assessment Out brief

RESULTS

Cyber Hygiene Activities

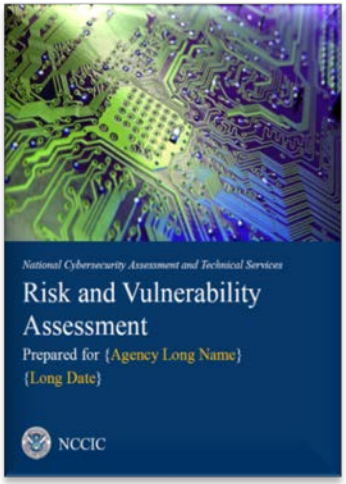
Scanning

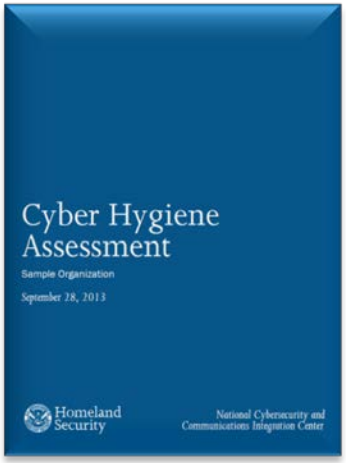
- Identify
  - *Active hosts, Operating System and Services*
  - *Vulnerabilities and weaknesses*
  - *Common configuration errors*
    - *Improperly signed Domains*
    - *Expired SSL Certificates*
- Understand how external systems and infrastructure appear to potential attackers

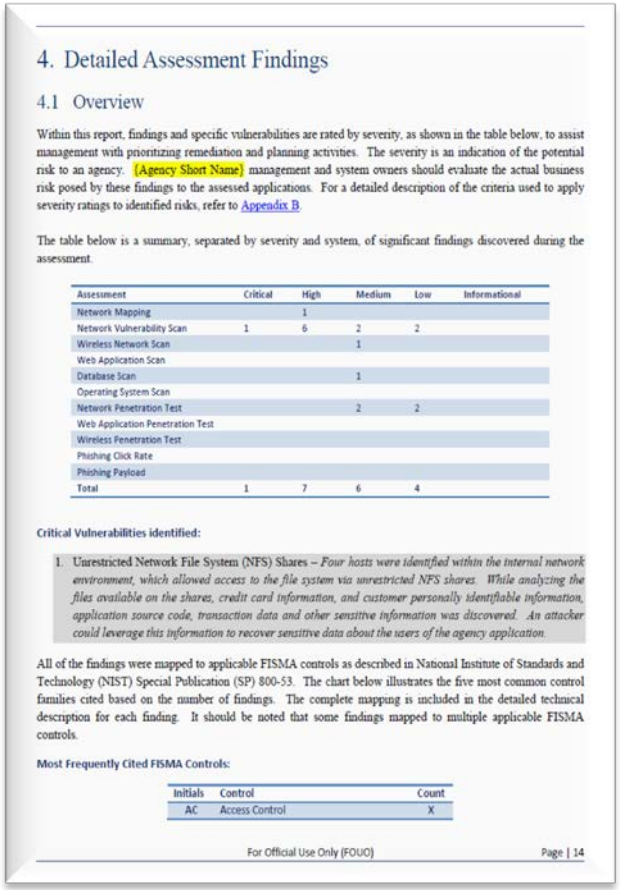
Past and Present Use

- Federal Response to Heartbleed
- OMB: M-15-01
  - *Identification of publicly available vulnerabilities*
- DHS Binding Operational Directive
- Individual Stakeholder persistent scans and exposure status
  - *2300+ Reports delivered this Fiscal Year*
  - *183 Stakeholders and growing*

Technical Output: Sample Snapshots







4. Detailed Assessment Findings

4.1 Overview

Within this report, findings and specific vulnerabilities are rated by severity, as shown in the table below, to assist management with prioritizing remediation and planning activities. The severity is an indication of the potential risk to an agency. {Agency Short Name} management and system owners should evaluate the actual business risk posed by these findings to the assessed applications. For a detailed description of the criteria used to apply severity ratings to identified risks, refer to Appendix B.

The table below is a summary, separated by severity and system, of significant findings discovered during the assessment.

Assessment	Critical	High	Medium	Low	Informational
Network Mapping		1			
Network Vulnerability Scan	1	6	2	2	
Wireless Network Scan			1		
Web Application Scan					
Database Scan			1		
Operating System Scan					
Network Penetration Test			2	2	
Web Application Penetration Test					
Wireless Penetration Test					
Phishing Click Rate					
Phishing Payload					
Total	1	7	6	4	

Critical Vulnerabilities identified:

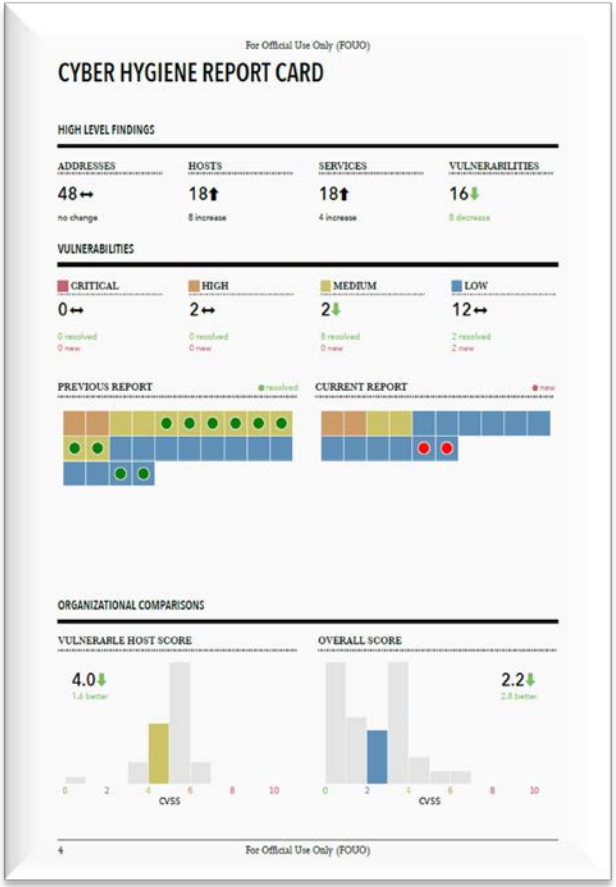
1. Unrestricted Network File System (NFS) Shares – *Four hosts were identified within the internal network environment, which allowed access to the file system via unrestricted NFS shares. While analyzing the files available on the shares, credit card information, and customer personally identifiable information, application source code, transaction data and other sensitive information was discovered. An attacker could leverage this information to recover sensitive data about the users of the agency application.*

All of the findings were mapped to applicable FISMA controls as described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. The chart below illustrates the five most common control families cited based on the number of findings. The complete mapping is included in the detailed technical description for each finding. It should be noted that some findings mapped to multiple applicable FISMA controls.

Most Frequently Cited FISMA Controls:

Initials	Control	Count
AC	Access Control	X

For Official Use Only (FOUO) Page | 14



For Official Use Only (FOUO)

CYBER HYGIENE REPORT CARD

HIGH LEVEL FINDINGS

ADDRESSES	HOSTS	SERVICES	VULNERABILITIES
48 ↔	18 ↑	18 ↑	16 ↓
no change	8 increase	4 increase	8 decrease

VULNERABILITIES

CRITICAL	HIGH	MEDIUM	LOW
0 ↔	2 ↔	2 ↓	12 ↔
0 resolved 0 new	0 resolved 0 new	8 resolved 0 new	2 resolved 2 new

PREVIOUS REPORT ● resolved CURRENT REPORT ● new

ORGANIZATIONAL COMPARISONS

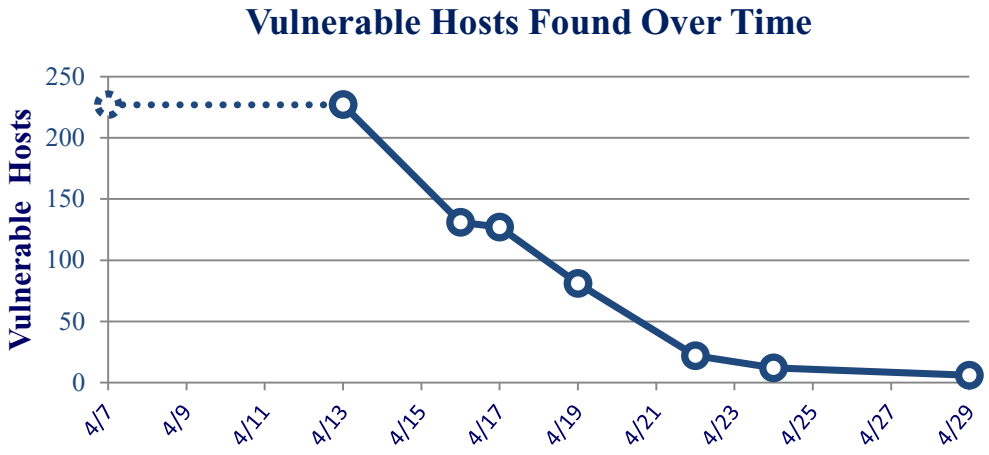
VULNERABLE HOST SCORE: 4.0 ↓ 1.6 better

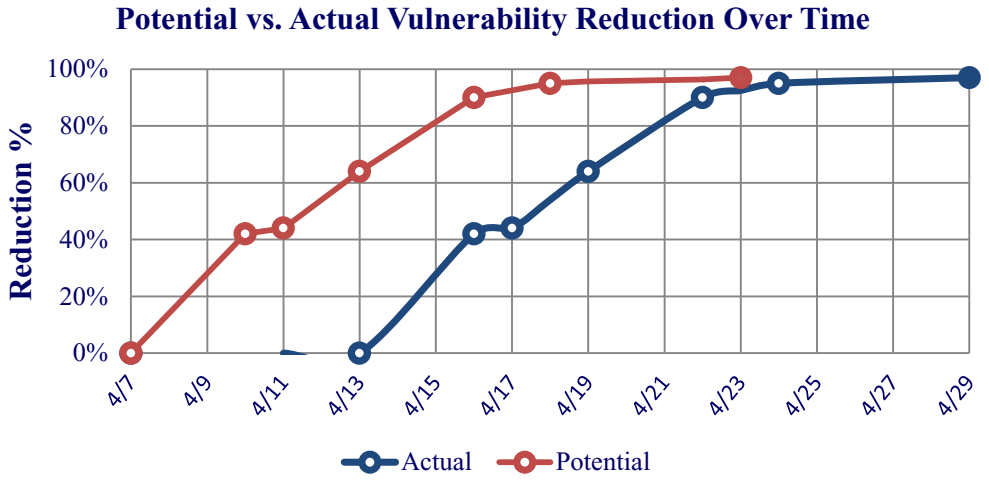
OVERALL SCORE: 2.2 ↓ 2.8 better

CVSS

4 For Official Use Only (FOUO)

Past Performance, Success Story: HeartBleed

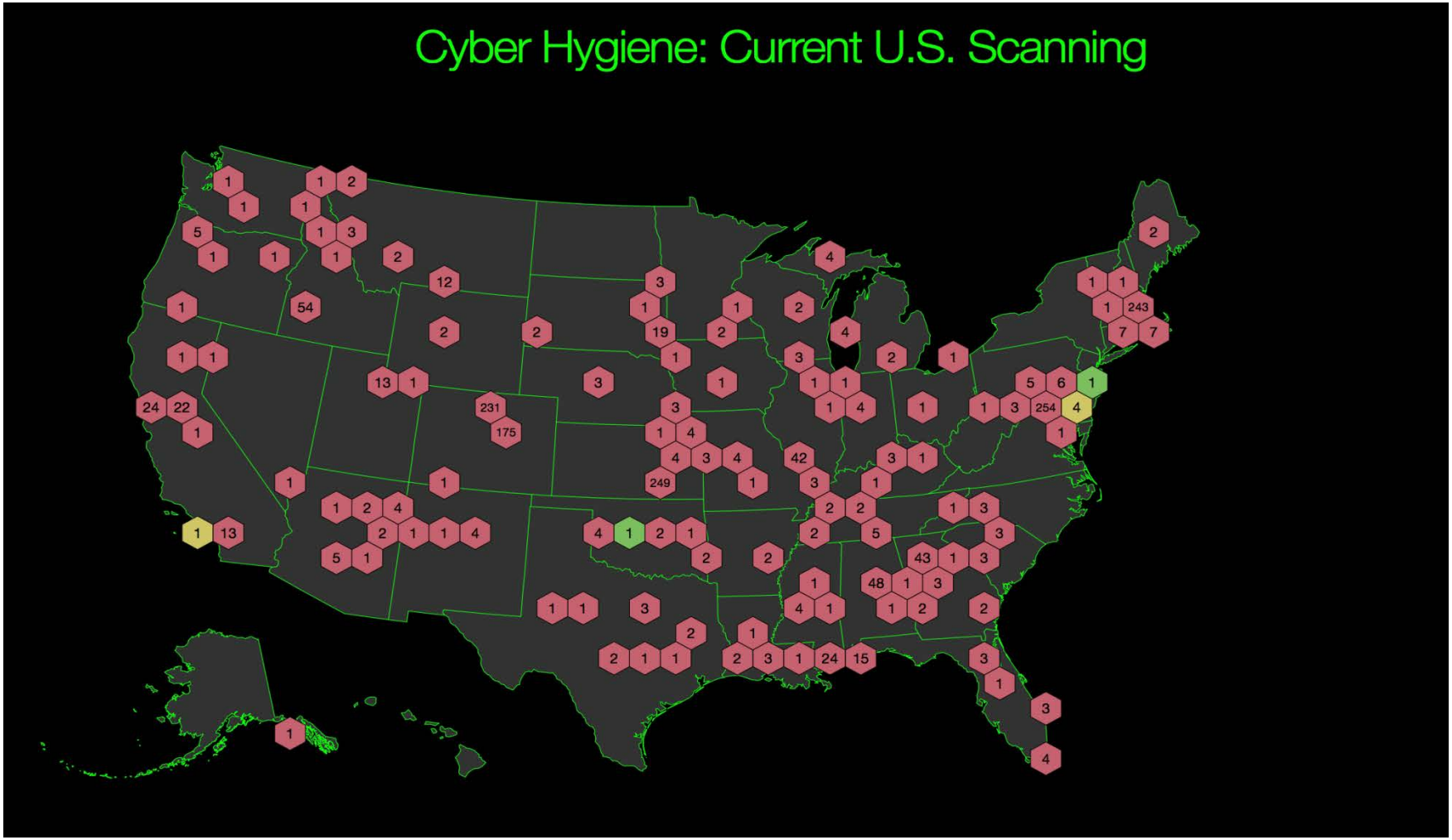




Notable Observations:

- DHS had the capability to initiate scanning immediately but was delayed due to a lack of authorization
- Observed 98% vulnerability reduction between first and last scan
- Had scanning started April 7th and achieved similar results the length of exposure could have been reduced by 29%

Visual 1: Current U.S. Scanning



Questions?

NCATS_INFO@hq.dhs.gov